



Strasbourg, 9 June 2008

CDMC(2008)004rev

**STEERING COMMITTEE ON  
THE MEDIA AND NEW COMMUNICATION SERVICES**

**(CDMC)**

---

**7th meeting  
27 to 30 May 2008  
Justizpalast, Vienna**

---

**Abridged Report**

---

---

*This document will not be distributed at the meeting. Please bring this copy.*

1. The Steering Committee on the Media and New Communication Services (CDMC) held its 7th meeting from 27 to 30 May in Vienna at the invitation of the Austrian government. The meeting was chaired by Mr Matthias TRAIMER (Austria). The agenda of the meeting, as adopted, appears in Appendix I.

### **Items requiring a decision by the Committee of Ministers**

2. *Guidelines to assist Internet Service Providers in their practical understanding of, and compliance with, key human rights and fundamental freedoms in the Information Society, in particular with regard to Article 10 of the European Convention on Human Rights:* The CDMC considered and approved the guidelines which were prepared by the Group of Specialists on Human Rights in the Information Society (MC-S-IS) in close cooperation with the European Internet Service Providers Association (EuroISPA). During the meeting the CDMC held an exchange of views with the President of EuroISPA.

The CDMC welcomed this close inter-governmental/industry cooperation, and reflected on the desirability for enhanced partnerships which will contribute to the effectiveness and impact of its work. It decided to pursue this reflection in the context of the preparation of the next specialised Conference of Ministers, seeking to develop a truly multi-stakeholder approach to media and Information Society standard-setting work.

**The Committee of Ministers is invited to take note of the above-mentioned Guidelines (cf. Appendix II).**

3. *Guidelines to assist online games providers in their practical understanding of, and compliance with, human rights and fundamental freedoms in the Information Society, in particular with regard to Article 10 of the European Convention on Human Rights:* The CDMC considered and approved the guidelines which were prepared by the MC-S-IS in close cooperation with Interactive Software Federation of Europe (ISFE). During the meeting, the CDMC held an exchange of views with the Secretary General of ISFE.

**The Committee of Ministers is invited to take note of the above-mentioned Guidelines (cf. Appendix III).**

4. *Possible future mechanism for promoting respect of Article 10 of the European Convention on Human Rights:* In response to the Committee of Minister's request following the Parliamentary Assembly Recommendations 1783(2007) on threats to the lives and freedom of expression for journalists and 1791(2007) on the state of human rights and democracy in Europe, the CDMC pursued consideration of this subject on the basis of a Bureau report on the state of discussions. While recognising that problems exist as regards respect for Article 10 of the Convention in member states, a tour de table during which 30 CDMC delegations took the floor, showed a majority of 14 to 12 against the establishment of a new monitoring mechanism.

**The CDMC therefore decided to ask the Committee of Ministers for further instructions on the subject.**

## **Items submitted to the Committee of Ministers for information**

*5. Possible Council of Europe Convention on the protection of the neighbouring rights of broadcasting organisations:* The CDMC welcomed the ad hoc terms of reference given to it by the Committee of Ministers on the subject, discussed the merits of elaborating a new convention (having regard to existing international instruments, including Council of Europe conventions, one of which has not entered into force for want of sufficient ratifications) and decided on the manner in which to proceed with this work. The CDMC will resume discussions on this matter at its next meeting.

*6. Media complaints bodies:* The CDMC reconsidered the approach to be followed, with a view to fulfilling the ad hoc terms of reference it received from the Committee of Ministers on 13 June 2007 “to examine and make recommendations on the operation and functioning of media complaints procedures and media complaints bodies established in member states, taking into account any difficulties faced by individuals and groups affected by statements in the media to obtain redress through these mechanisms”. It decided that, resources permitting, a consultant be asked to prepare an analysis of existing mechanisms and that a round table be organised with representatives of media complaint bodies, professional organisations and other relevant actors. This will help decide on further action to be taken and elaborate recommendations on the subject as requested by the Committee of Ministers.

*7. Work of the CDMC’s subordinate bodies:* The CDMC took note of the ongoing work of its groups of specialists and of the reports of their last meetings. The CDMC also held an exchange of views with Ms Bissera Zankova (Bulgaria), coordinating the “living together” project and work on media in times of crisis and took note of the progress made in that respect. The CDMC noted in particular that a thematic study on developments in national legislation since 2001 concerning the fight against terrorism which have a bearing on freedom of expression and information and freedom of the media will be completed by mid-September 2008. It decided that, resources permitting, a conference be organised to explore with media professionals the impact of the legal developments in practice. This will permit to identify further action required.

The CDMC welcomed the adoption of the White Paper on Intercultural Dialogue and decided to have an item on this subject regularly on its agenda. It also noted the launching, on the occasion of World Press Freedom Day, on 3 May 2008, of a web-based forum on rights and responsibilities of media and the working conditions of journalists in times of crisis.

*8. Exchange of views with Mr Miklos Haraszti, OSCE Representative on Freedom of the Media:* During this exchange, Mr Haraszti reiterated his call for decriminalisation, or at least “deprisonisation”, of defamation in Council of Europe member states, including those countries which do not use existing criminal law provisions to retribute journalists’ professional conduct or mistakes. The OSCE Representative on Freedom of the Media also expressed support for the establishment of a specialised Council of Europe monitoring mechanism capable of contributing to the effectiveness in practice of the organisation’s valuable minimum standards on media and freedom of expression.

*9. Internet governance and implementation of WSIS action lines:* The CDMC exchanged views on the Council of Europe’s participation and contribution to the UN-led Internet Governance Forum (IGF) and the World Summit on the Information Society action lines. Building on its successful input of 2007, the Council of Europe should continue to place the

values and standards of the Organisation at the forefront of developments in the information society and give them an even wider visibility. The CDMC encouraged the Secretariat to organise a European preparatory meeting in anticipation of the December 2008 IGF, as suggested by some member States.

*10. First Council of Europe Conference of Specialised Ministers responsible or in charge of Media and New Communication Services (to be held in Reykjavik, on 28 and 29 May 2009):* The CDMC pursued discussions on a draft programme, possible key note speakers, moderators and panellists. It also started considering items for the elaboration of texts, in particular a draft action plan, for possible adoption at the Conference. The Conference will focus on a new notion of media and the resulting standard-setting requirements, consolidation/effectiveness of media-related Council of Europe standards and on the Council of Europe's vision of Internet governance.

*11. Request for observer status:* The CDMC examined the request by the non-governmental organisation Association of European Journalist (AEJ) to be given observer status with the CDMC. The CDMC decided in favour of this request.

*12. Work of other Council of Europe bodies:* The CDMC took note of the work of relevant Council of Europe bodies. It observed that there is an increasing number of requests for the CDMC to take part in meetings of, or other events organised by, those bodies given the attention being paid by them to media-related matters. The CDMC decided that, resources permitting, a favourable response should be given to relevant invitations and discussed ways of rationalising participation (early information on upcoming meetings/events, elaboration of a list of CDMC members available to attend such meetings/events and indicating their areas of interest/expertise, reporting back).

*13. Other issues:* The CDMC took note of progress on the revision of the European Convention on Transfrontier Television (CETS No.:132) and on work being carried out on the European Convention on the legal protection of services based on, or consisting of conditional access (ECCA). The representative of Slovenia informed the CDMC of the work of the current presidency of the European Union related to the media and the new communication services.

**APPENDIX I - AGENDA**

- 1. Opening of the meeting**
- 2. Adoption of the agenda**
- 3. Decisions of the Committee of Ministers of interest to the work of the CDMC**
- 4. Request for observer status by NGO**
- 5. Work programme for the CDMC in 2008-2009**
- 6. Promoting visibility of the work of the CDMC**
- 7. Draft instruments or texts for consideration by the CDMC**
- 8. Implementation of Council of Europe standards on media and freedom of expression prepared under the authority of the CDMC**
- 9. Discussion on a possible future mechanism in respect of Article 10 of the European Convention on Human Rights**
- 10. Discussion on a possible Council of Europe convention on the protection of the neighbouring rights of broadcasting organisations**
- 11. Ongoing work of the CDMC and its subordinate bodies**
- 12. Work on media in times of crisis and on inter-cultural dialogue**
- 13. Internet Governance and implementation of WSIS action lines**
- 14. Council of Europe Conference of Ministers responsible for the Media and New Communication Services (Reykjavik, 28-29 May 2009)**
- 15. Standing Committee on Transfrontier Television (T-TT)**
- 16. Information on the work of, and co-operation with, other Council of Europe bodies, of interest to the CDMC**
- 17. Other information of interest to the work of the CDMC**
- 18. Administrative and budgetary matters**
- 19. Dates of the next meeting**
- 20. Items to be included on the agenda of the 8th meeting of the CDMC**
- 21. Other business**
- 22. Abridged report**

## APPENDIX II

### **Guidelines to assist Internet Service Providers in their practical understanding of, and compliance with, key human rights and fundamental freedoms in the Information Society, in particular with regard to Article 10 of the European Convention on Human Rights**

#### **Background and context**

1. As part of its terms of reference, the Group of Specialists on Human Rights in the Information Society (MC-S-IS) was instructed by the Steering Committee on the Media and New Communications Services (CDMC) to develop tools to assist key state and non-state actors in their practical understanding of, and compliance with, human rights and fundamental freedoms in the information society, in particular with regard to Article 10 of the European Convention on Human Rights.
2. In response to its terms of reference, the MC-S-IS decided to develop human rights guidelines addressed to key actors with the aim of providing simple and practical advice relevant to the day-to-day activities of certain key actors, in this case Internet Service Providers (ISPs).
3. To strengthen the practical nature of the guidelines, the MC-S-IS established contact with and has cooperated closely with EuroISPA, the European Internet Service Providers' Association. EuroISPA has commented on the draft guidelines at various stages of their development and a meeting with participation of representatives of EuroISPA, Austrian ISPs as well as Council of Europe experts and Secretariat was organised. Moreover, EuroISPA was represented during the discussions of the draft guidelines at the 9th meeting of the MC-S-IS. The MC-S-IS aims to continue this positive co-operation after the text is finalised to maximise the impact and awareness of the guidelines among ISPs.
4. Based on existing Council of Europe standard-setting instruments, these guidelines are different from the existing Council of Europe instruments by being addressed directly to ISPs in order to raise awareness of the human rights aspects of their day-to-day work and activities. They are not binding on ISPs, rather they are a source of information and guidance for them to deal with practical issues concerning privacy, security and freedom of expression.
5. The guidelines are divided into three parts: (i) the role and position of ISPs vis-à-vis human rights in the information society; (ii) practical guidelines for ISPs containing advice and assistance; (iii) extracts from Council of Europe standard setting documents relevant to ISPs.

#### **Human rights guidelines for Internet Service Providers**

Everyone has the right to freedom of expression and information. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Article 10 of the European Convention on Human Rights

Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 of the European Convention on Human Rights

### **Understanding the role and position of Internet Service Providers in respecting and promoting human rights**

6. Internet Service Providers (ISPs), in providing the basic infrastructure and the basic services that allow users to access and use the Internet and thereby exercise their rights to benefit from the information society, deliver services with a significant public service value to society.

7. ISPs have a unique position and possibility to promote the exercise of and respect for human rights and fundamental freedoms. In addition, the provision of Internet services is increasingly becoming a prerequisite for a comprehensive participatory democracy. ISPs also play an important role vis-à-vis states which are committed to protecting and promoting these rights and freedoms as part of their international law obligations.

8. ISPs provide a variety of services to their customers, be it as access-providers or as providers of other information society services (application-providers, content-providers and/or host-providers). It is recognised in these guidelines that not all ISPs have the same roles and responsibilities vis-à-vis users but that these may depend on the types of services the ISP delivers and what segment of customers the ISP serves.

9. Access-providers facilitate entry to the Internet and therefore to a diversity of information, culture and languages; they are often the first point of contact and trust for users. Their role is a prerequisite for enabling and empowering users to access the benefits of the information society, in particular to seek and impart information and ideas, to create and to access knowledge and education.

10. Access-providers, in particular those serving home-users and families, can be seen as fulfilling a part public service role that promotes their customers' rights to benefit from the information society and, to this end, strengthen the exercise and enjoyment of their rights and freedoms.

11. Equally, to the extent that access-providers and particularly host-providers may enforce decisions and actions with regard to the accessibility of services (e.g. remove, block or filter content), this can impact on rights and freedoms.

12. ISPs have access to varying amounts of information (content and/or traffic data) which underlines their important role and position vis-à-vis the rights and freedoms of users. ISPs should not be put under a general obligation to actively monitor content and traffic data; however there may be specific cases defined by law and upon specific orders where an ISP may need to assist in monitoring content or data or impart information about a user to a third party. Such cases could have an impact on freedom of expression or the right to private life.

13. Overall, there is considerable potential for ISPs, particularly host and content providers, to promote the opportunities and benefits of the information society, and this should be underlined and communicated to users, to states and, most importantly, to ISPs themselves.

14. In this regard, ISPs are encouraged to take note of, discuss and make their best efforts to comply with the following guidelines (overleaf) and to consider making reference to them on their websites and in their end-user agreements.

15. ISPs, in co-operation with associations of ISPs, member states, and, where appropriate, with the assistance of the Council of Europe, are also encouraged to make key personnel in their organisations aware of these guidelines and the issues raised therein.

16. Associations of ISPs can play an important role by assuming collective responsibility with regard to raising awareness and providing information about the issues raised in these guidelines. They are encouraged to actively promote these guidelines among their members, for instance by making reference to or incorporating them in their own codes of conduct and by providing expert knowledge.

17. As regards the information that should be provided towards customers, ISPs may choose to provide this information via associations of ISPs, particularly in the case of small enterprises and in those cases where the information is not provider-specific (such as information about risks on the Internet). Associations of ISPs can furthermore contribute to a harmonisation of user information and aggregate knowledge as regards the issues raised in the guidelines. In addition they can provide for cooperation and exchange of knowledge with existing structures in the field of Internet safety, such as the European Union Safer Internet Plus Programme.

18. The guidelines are without prejudice to and must be read in conjunction with the obligations applicable to ISPs and their activities under national, European and international law.



### Scope of these guidelines:

19. The following guidelines are grouped in several chapters, according to the respective roles of the ISPs. The first chapter applies to Internet access providers (providers of on-demand or dedicated Internet access services). The second chapter applies to providers of other information society services, such as is the case for providers of hosting services, content providers and application providers. The third chapter applies to all Internet service providers accordingly.

20. The guidelines do not apply to mere transit providers.

## **Guidelines**

### Guidelines for ISPs providing access services:

- 21. Ensure that your customers have access to information about potential risks to their rights, security and privacy online, including information on what you are doing to help your customers counter those risks. Provide information about available tools and software that your customers may use to protect themselves further. If you provide this information yourself, ensure that it is provided in the most accurate, accessible and up-to-date way possible. If you do not provide this information yourself, link your customers to adequate information resources, particularly those of associations of ISPs or networks in the field of Internet safety. In particular information on the following risks could be made available:

#### 21.1 Illegal and/or harmful content, risks for children:

- Provide information or link to information about risks of encountering or contributing to the dissemination of illegal content on the Internet as well as the risks for children of being exposed to harmful content or behaviour when they are online. The latter may include content or behaviour capable of adversely affecting the physical, emotional and psychological well-being of children, such as online pornography, the portrayal and glorification of violence and self-harm, demeaning, discriminatory or racist expressions or apologia for such conduct, solicitation (grooming), bullying, stalking and other forms of harassment. Although you will not be expected to advise on what content or behaviours are illegal and/or harmful, the information you give could usefully include:
  - explanations on what you are doing to counter such content and behaviour, particularly your cooperation with hotlines against illegal content (e.g. Inhope);
  - guidance on how users can protect themselves against the risks of encountering illegal and/or harmful content and behaviour (e.g. by linking them to relevant information on Internet safety websites);
  - information on available software tools designed to protect users against illegal and/or harmful content, including information about how the tools work and can be adapted by the users to meet their individual needs.

- Provide information or link to information on what your customers can do to protect their children online. Make reference to websites with child-friendly content and to available online safety resources such as the Council of Europe Internet Literacy Handbook ([www.coe.int/internet-literacy](http://www.coe.int/internet-literacy)), the Council of Europe online game “Through the Wild Web Woods” ([www.wildwebwoods.org](http://www.wildwebwoods.org)) or websites of Internet safety nodes ([www.saferinternet.org](http://www.saferinternet.org)).

### 21.2 Security risks:

- If appropriate, explain what you are doing to protect your customers against security risks. Such risks may concern data integrity (viruses, worms, trojans, etc.), confidentiality (e.g. when making transactions online), network security or other risks (e.g. phishing).
- Raise your customers’ awareness or link your customers to further information on how to counter risks to their security on the Internet.

### 21.3 Privacy risks:

- Provide for information or link to information about potential risks of customers to their privacy when using the Internet. Such risks may concern the hidden collection, recording and processing of data (spyware, profiling). If appropriate, link to websites of your national authorities with available information of applicable laws on privacy and protection of personal data.
  - Offer further information and guidance to your customers about the technical means which they may use to protect themselves against privacy risks (anti-spyware tools etc.).
- 22. When your customers need support in dealing with the risks identified above, ensure that they can either make further enquiries in the appropriate form (e.g. telephone, e-mail, writing, personal contact) or link them to appropriate information resources.
  - 23. Be careful about blocking or degrading the quality of your services for the use of certain applications or software based on a given technical protocol. If you apply bandwidth caps, filter or block certain traffic, make sure that your customers are informed about such service restrictions in a clear manner beforehand.
  - 24. Cutting access to individual customer accounts constitutes a restriction on your customer’s rights to access the benefits from the information society and to exercise their rights to freedom of expression and information. Cutting access should only be done for law enforcement or other legitimate and strictly necessary reasons, such as a violation of contractual obligations or intentional abuse, while having regard to legal safeguards that may be applicable under national law. The customer should, where appropriate, be properly warned and informed beforehand, be given adequate reasons for the cutting of access and be instructed of the steps to be taken to re-establish the access.

Guidelines for ISPs providing other information society services (hosting, applications and content):

- 25. Make sure any filtering or blocking of services carried out is legitimate, proportional and transparent to your customers in accordance with the Council of Europe Recommendation on measures to promote the respect for freedom of expression and information with regard to Internet filters, CM/Rec(2008)6. Inform your customers of any filtering or blocking software installed on your servers that may lead to a removal or inaccessibility of content as well as the nature of the filtering that takes place (form of filtering, general criteria used to filter, reasons for applying filters).
- 26. In respect of filtering, blocking or removal of illegal content, you should do so only after a verification of the illegality of the content, for instance by contacting the competent law enforcement authorities. Acting without first checking and verifying may be considered as an interference with legal content and with the rights and freedoms of those creating, communicating and accessing such content, in particular the right to freedom of expression and information.
- 27. Inform your customers about your general policy dealing with complaints on alleged illegal content you might be hosting. Give clear indications to the general public on how to complain, and to your customers on how to respond to such complaints.
- 28. If you provide your customers with specific application services, such as the use of chat, e-mail, blogs etc., you should take care to ensure the use of the applications is as safe as possible and that your customers are made aware of the way the applications work. When providing facilities such as chat rooms or discussion forums, make sure that clear rules for user registration and use of nicknames are established and that users are informed about the rules in a clear manner before they start using your services.
- 29. Although you will not be expected to provide advice on what content or behaviours are illegal and/or harmful, you could usefully give information to teachers and parents on risks to children when using application services provided by you (chat rooms, messageboards etc.), in particular the risks of encountering harmful content or behaviour (grooming, bullying, etc.) when using your services.
- 30. When providing applications for e-mailing to your customers make sure that any measures you provide, such as spam-recognition or spam-filtering software, are effective (recognising or filtering spam while not interfering with legitimate e-mails) and your customers are properly informed about their functionality and methodology as well as the possibility to adapt their configuration.
- 31. If you provide content services to your customers, such as web-based information or news services, consider offering users a right of reply allowing the rapid correction of incorrect information along the lines of the minimum principles contained in the Council of Europe Recommendation (2004)16 on the right of reply in the new media environment.

Guidelines for ISPs with regard to the right to respect for private life and data protection:

- 32. Establish appropriate procedures and use available technologies to protect the privacy of users and secrecy of content and traffic data, especially by ensuring data

integrity, confidentiality as well as physical and logical security of the network and of the services provided over the network. The level of protection should be adapted to the type of service you provide accordingly.

- 33. Offer further information and guidance to your customers about the technical means they may use to protect themselves against security risks to data and communications (such as anti-spyware software tools, firewalls, encryption technology or digital signatures etc.).
- 34. When acting with regard to the communications of users (for example by allowing the interception or monitoring of users' e-mails) such action should only be undertaken in case of a legal duty to do so, on specific orders or instructions from a competent public authority made in accordance with the law. Do not actively monitor the content of communications on your network. Furthermore, the deletion and modification of the user's correspondence (e.g. by spam-filters) should depend on the explicit consent of the user before the spam-filter etc. is activated.
- 35. Do not to reveal the identity of users, their traffic data or the content of data accessed by them to a third party, unless under a legal duty to do so or following specific orders or instructions from the competent public authority made in accordance with the law. Requests in this respect brought to you from abroad should be handled through the competent authorities in your country.
- 36. Inform your customers in which circumstances you are under a legal duty to reveal their identification, connection or traffic data by request from law enforcement agencies etc. Such information could particularly be provided by associations of ISPs to whom you might want to link. If you receive a request to disclose such data, make sure to check the authenticity of the request and that it is made by a competent authority in accordance with the law.
- 37. Do not to collect, process or store data about users, unless this is necessary for explicit, specified and legitimate purposes in accordance with data protection laws. Do not store data for longer than required by law or than is necessary to achieve the purpose of processing of the data.
- 38. Do not use personal data on users for your own promotional or marketing purposes unless the user concerned, after having been informed, has given his or her consent and this consent has not been revoked. Do not make personal data publicly available! Such publication may infringe other people's privacy and may also be prohibited by law.

## Appendix I

### Extracts from existing Council of Europe standards relevant to the roles and responsibilities of ISPs

#### **Recommendation No. R(99)5 of the Committee of Ministers to member states for the protection of privacy on the Internet<sup>1</sup>**

Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways which may be incorporated in or annexed to codes of conduct

#### III. For Internet service providers

1. Use appropriate procedures and available technologies, preferably those which have been certified, to protect the privacy of the people concerned (even if they are not users of the Internet), especially by ensuring data integrity and confidentiality as well as physical and logical security of the network and of the services provided over the network.
2. Inform users of privacy risks presented by use of the Internet before they subscribe or start using services. Such risks may concern data integrity, confidentiality, the security of the network or other risks to privacy such as the hidden collection or recording of data.
3. Inform users about technical means which they may lawfully use to reduce security risks to data and communications, such as legally available encryption and digital signatures. Offer such technical means at a cost-oriented price, not a deterrent price.
4. Before accepting subscriptions and connecting users to the Internet, inform them about the possibilities of accessing the Internet anonymously, and using its services and paying for them in an anonymous way (for example, pre-paid access cards). Complete anonymity may not be appropriate because of legal constraints. In those cases, if it is permitted by law, offer the possibility of using pseudonyms. Inform users of programmes allowing them to search and browse anonymously on the Internet. Design your system in a way that avoids or minimises the use of personal data.
5. Do not read, modify or delete messages sent to others.
6. Do not allow any interference with the contents of communications, unless this interference is provided for by law and is carried out by a public authority.
7. Collect, process and store data about users only when necessary for explicit, specified and legitimate purposes.
8. Do not communicate data unless the communication is provided for by law .
9. Do not store data for longer than is necessary to achieve the purpose of processing.

---

<sup>1</sup> Adopted on 23 February 1999.

10. Do not use data for your own promotional or marketing purposes unless the person concerned, after having been informed, has not objected or, in the case of processing of traffic data or sensitive data, he or she has given his or her explicit consent.

11. You are responsible for proper use of data. On your introductory page highlight a clear statement about your privacy policy. This statement should be hyperlinked to a detailed explanation of your privacy practice. Before the user starts using services, when he or she visits your site, and whenever he or she asks, tell him or her who you are, what data you collect, process and store, in what way, for what purpose and for how long you keep them. If necessary, ask for his or her consent. At the request of the person concerned, correct inaccurate data immediately and delete them if they are excessive, out of date or no longer required and stop the processing carried out if the user objects to it. Notify the third parties to whom you have communicated the data of any modification. Avoid the hidden collection of data.

12. Information provided to the user must be accurate and kept up to date.

13. Think twice about publishing data on your site! Such publication may infringe other people's privacy and may also be prohibited by law.

14. Before you send data to another country seek advice, for example from the competent authorities in your country, on whether the transfer is permissible. You may have to ask the recipient to provide safeguards necessary to ensure protection of the data.

### **Declaration of the Committee of Ministers on freedom of communication on the Internet<sup>2</sup>:**

#### *Principle 6 - Limited liability of service providers for Internet content*

Member states should not impose on service providers a general obligation to monitor content on the Internet to which they give access, that they transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity.

Member states should ensure that service providers are not held liable for content on the Internet when their function is limited, as defined by national law, to transmitting information or providing access to the Internet.

In cases where the functions of service providers are wider and they store content emanating from other parties, member states may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information.

When defining under national law the obligations of service providers as set out in the previous paragraph, due care must be taken to respect the freedom of expression of those who made the information available in the first place, as well as the corresponding right of users to the information.

---

<sup>2</sup> Adopted on 28 May 2003.

In all cases, the above-mentioned limitations of liability should not affect the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of the law.

- **Extracts from the Explanatory memorandum to the Declaration on freedom of communication on the Internet:**

*Principle 6 - Limited liability of service providers for Internet content*

Here it is established that as a general rule intermediaries in the communication chain should not be held liable for content transmitted through their services, except in certain limited circumstances. Along the lines of Articles 12-15 of the Directive on electronic commerce, the exemptions to liability take into account the different types of activities of the intermediaries, namely providing access to communication networks, transmitting data and hosting information. The degree of liability depends on the possibilities of service providers to control the content and whether they are aware of its illegal nature. The limitations on liability do not apply if intermediaries intentionally disseminate illegal content.

*1st paragraph - no general obligation to monitor*

This paragraph is based on Article 15 of the Directive on electronic commerce. Member States should not impose any general obligation on service providers to monitor the information on the Internet to which they give access, that they transmit or store. Nor should they be subject to a general obligation to actively seek facts or circumstances indicating illegal activity, since this might have the effect of curbing freedom of expression.

This paragraph of Principle 6 does not prevent public authorities in member States from obliging service providers in certain cases, for example during a criminal investigation, to monitor the activities of their clients.

*2nd paragraph - “mere conduit”*

In the case of mere transmission of information or providing access to communication networks, intermediaries should not be held liable for illegal content. When the role of intermediaries goes beyond that, in particular when they initiate the transmission, select the receiver of the transmission or select or modify the information transmitted, their liability may be invoked.

The activity of the intermediary which is at stake here, and which should be exempt from liability, is sometimes referred to as “mere conduit” (cf. Article 12 of the Directive on electronic commerce).

*3rd paragraph - “hosting”*

In the case of hosting content emanating from third parties, intermediaries should in general not be held liable (cf. Article 14 of the Directive on electronic commerce). This does not apply, however, when the third party is acting under the control of the intermediary, for example when a newspaper company has its own server to host content produced by its journalists. However, if the host becomes aware of the illegal nature of the content on its

servers or, in the event of a claim for damages, of facts revealing an illegal activity, it may reasonably be held liable. The precise conditions should be laid down in national law.

*4th paragraph - "notice and take down" procedures and freedom of expression and information*

As stipulated in paragraph 3 of Principle 6 of the Declaration, service providers may be held liable if they do not act expeditiously to remove or disable access to information or services when they become aware, as defined by national law, of their illegal nature. It is to be expected that member States will define in more detail what level of knowledge is required of service providers before they become liable. In this respect, so-called "notice and take down" procedures are very important. Member States should, however, exercise caution imposing liability on service providers for not reacting to such a notice. Questions about whether certain material is illegal are often complicated and best dealt with by the courts. If service providers act too quickly to remove content after a complaint is received, this might be dangerous from the point of view of freedom of expression and information. Perfectly legitimate content might thus be suppressed out of fear of legal liability.

*5th paragraph - the possibility of issuing injunctions remains intact*

It is highlighted here, in line with Articles 12-14 of the Directive on electronic commerce, that despite the above-mentioned limitations of liability, the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of law, remains intact.

**Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society<sup>3</sup>**

With regard to self- and co-regulatory measures which aim to uphold freedom of expression and communication, private sector actors are encouraged to address in a decisive manner the following issues:

private censorship (hidden censorship) by Internet service providers, for example blocking or removing content, on their own initiative or upon the request of a third party;

**Recommendation No. Rec(2007)11 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment<sup>4</sup>**

Member states, the private sector and civil society are encouraged to develop common standards and strategies to promote transparency and the provision of information, guidance and assistance to the individual users of technologies and services, in particular in the following situations:

...

vii. the removal of content deemed to be illegal with regard to the rule of law considerations;

**Recommendation No. Rec (2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet<sup>5</sup>**

---

<sup>3</sup> Adopted on 13 May 2005.

<sup>4</sup> Adopted on 26 September 2007.



Member states should adopt or develop policies to preserve and, whenever possible, enhance the protection of human rights and respect for the rule of law in the information society. In this regard, particular attention should be paid to:

- the right to private life and private correspondence on the Internet and in the use of other ICTs, including the respect for the will of users not to disclose their identity, promoted by encouraging individual users and Internet service and content providers to share the responsibility for this;

Member states should promote public discussion on the responsibilities of private actors, such as Internet service providers, content providers and users, and encourage them - in the interests of the democratic process and debate and the protection of the rights of others - to take self-regulatory and other measures to optimise the quality and reliability of information on the Internet and to promote the exercise of professional responsibility, in particular with regard to the establishment, compliance with, and monitoring of the observance of codes of conduct.

**Recommendation No. CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters**

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve greater unity between its members for the purpose of safeguarding and realising the ideals and principles which are their common heritage;

Recalling that States Parties to the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights – ETS No. 5) have undertaken to secure to everyone within their jurisdiction the human rights and fundamental freedoms defined in the Convention;

Reaffirming the commitment of member states to the fundamental right to freedom of expression and to receive and impart information and ideas without interference by public authorities and regardless of frontiers, as guaranteed by Article 10 of the European Convention on Human Rights;

Aware that any intervention by member states that forbids access to specific Internet content may constitute a restriction on freedom of expression and access to information in the online environment and that such a restriction would have to fulfil the conditions in Article 10, paragraph 2, of the European Convention on Human Rights and the relevant case law of the European Court of Human Rights;

Recalling in this respect the Declaration on human rights and the rule of law in the information society, adopted by the Committee of Ministers on 13 May 2005, according to which member states should maintain and enhance legal and practical measures to prevent state and private censorship;

---

<sup>5</sup> Adopted on 7 November 2007.

Recalling Recommendation Rec(2007)11 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment, according to which member states, the private sector and civil society are encouraged to develop common standards and strategies to promote transparency and the provision of information, guidance and assistance to the individual users of technologies and services concerning, *inter alia*, the blocking of access to and filtering of content and services with regard to the right to receive and impart information;

Noting that the voluntary and responsible use of Internet filters (products, systems and measures to block or filter Internet content) can promote confidence and security on the Internet for users, in particular children and young people, while also aware that the use of such filters can impact on the right to freedom of expression and information, as protected by Article 10 of the European Convention on Human Rights;

Recalling Recommendation [Rec\(2006\)12](#) of the Committee of Ministers on empowering children in the new information and communications environment, which underlines the importance of information literacy and training strategies for children to enable them to better understand and deal with content (for example violence and self-harm, pornography, discrimination and racism) and behaviours (such as grooming, bullying, harassment or stalking) carrying a risk of harm, thereby promoting a greater sense of confidence, well-being and respect for others in the new information and communications environment;

Convinced of the necessity to ensure that users are made aware of, understand and are able to effectively use, adjust and control filters according to their individual needs;

Recalling Recommendation [Rec\(2001\)8](#) of the Committee of Ministers on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), which encourages the neutral labelling of content to enable users to make their own value judgements over such content and the development of a wide range of search tools and filtering profiles, which provide users with the ability to select content on the basis of content descriptors;

Aware of the public service value of the Internet, understood as people's significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions, entertainment) and the resulting legitimate expectation that Internet services be accessible, affordable, secure, reliable and ongoing and recalling in this regard Recommendation Rec(2007)16 of the Committee of Ministers on measures to promote the public service value of the Internet;

Recalling the Declaration of the Committee of Ministers on freedom of communication on the Internet of 28 May 2003, which stresses that public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers, but that this does not prevent the installation of filters for the protection of minors, in particular in places accessible to them, such as schools or libraries;

Reaffirming the commitment of member states to everyone's right to private life and secrecy of correspondence, as protected by Article 8 of the European Convention on Human Rights, and recalling the Convention for the Protection of Individuals with regard to Automatic

Processing of Personal Data (ETS No. 108) and its Additional Protocol regarding supervisory authorities and transborder data flows (ETS No. 181) as well as Recommendation No. R (99) 5 of the Committee of Ministers on the protection of privacy on the Internet,

Recommends that member states adopt common standards and strategies with regard to Internet filters to promote the full exercise and enjoyment of the right to freedom of expression and information and related rights and freedoms in the European Convention on Human Rights, in particular by:

- taking measures with regard to Internet filters in line with the guidelines set out in the appendix to this recommendation;
- bringing these guidelines to the attention of all relevant private and public sector stakeholders, in particular those who design, use (install, activate, deactivate and implement) and monitor Internet filters, and to civil society, so that they may contribute to their implementation.

#### *Appendix to Recommendation CM/Rec(2008)6*

##### *Guidelines*

#### I. Using and controlling Internet filters in order to fully exercise and enjoy the right to freedom of expression and information

Users' awareness, understanding of and ability to effectively use Internet filters are key factors which enable them to fully exercise and enjoy their human rights and fundamental freedoms, in particular the right to freedom of expression and information, and to participate actively in democratic processes. When confronted with filters, users must be informed that a filter is active and, where appropriate, be able to identify and to control the level of filtering the content they access is subject to. Moreover, they should have the possibility to challenge the blocking or filtering of content and to seek clarifications and remedies.

In co-operation with the private sector and civil society, member states should ensure that users are made aware of activated filters and, where appropriate, are able to activate and deactivate them and be assisted in varying the level of filtering in operation, in particular by:

- i. developing and promoting a minimum level of information for users to enable them to identify when filtering has been activated and to understand how, and according to which criteria, the filtering operates (for example, black lists, white lists, keyword blocking, content rating, etc., or combinations thereof);
- ii. developing minimum levels of and standards for the information provided to the user to explain why a specific type of content has been filtered;
- iii. regularly reviewing and updating filters in order to improve their effectiveness, proportionality and legitimacy in relation to their intended purpose;
- iv. providing clear and concise information and guidance regarding the manual overriding of an activated filter, namely whom to contact when it appears that content has been

unreasonably blocked and the reasons which may allow a filter to be overridden for a specific type of content or Uniform Resource Locator (URL);

v. ensuring that content filtered by mistake or error can be accessed without undue difficulty and within a reasonable time;

vi. promoting initiatives to raise awareness of the social and ethical responsibilities of those actors who design, use and monitor filters with particular regard to the right to freedom of expression and information and to the right to private life, as well as to the active participation in public life and democratic processes;

vii. raising awareness of the potential limitations to freedom of expression and information and the right to private life resulting from the use of filters and of the need to ensure proportionality of such limitations;

viii. facilitating an exchange of experiences and best practices with regard to the design, use and monitoring of filters;

ix. encouraging the provision of training courses for network administrators, parents, educators and other people using and monitoring filters;

x. promoting and co-operating with existing initiatives to foster responsible use of filters in compliance with human rights, democracy and the rule of law;

xi. fostering filtering standards and benchmarks to help users choose and best control filters.

In this context, civil society should be encouraged to raise users' awareness of the potential benefits and dangers of filters. This should include promoting the importance and significance of free and unhindered access to the Internet so that every individual user may fully exercise and enjoy their human rights and fundamental freedoms, in particular the right to freedom of expression and information and the right to private life, as well as to effectively participate in public life and democratic processes.

## II. Appropriate filtering for children and young people

The Internet has significantly increased the number and diversity of ideas, information and opinions which people may receive and impart in the fulfilment of their right to freedom of expression and information without interference by public authorities and regardless of frontiers. At the same time, it has increased the amount of readily available content carrying a risk of harm, particularly for children and young people. To satisfy the legitimate desire and duty of member states to protect children and young people from content carrying a risk of harm, the proportionate use of filters can constitute an appropriate means of encouraging access to and confident use of the Internet and be a complement to other strategies on how to tackle harmful content, such as the development and provision of information literacy.

In this context, member states should:

i. facilitate the development of strategies to identify content carrying a risk of harm for children and young people, taking into account the diversity of cultures, values and opinions;

- ii. co-operate with the private sector and civil society to avoid over-protection of children and young people by, *inter alia*, supporting research and development for the production of “intelligent” filters that take more account of the context in which the information is provided (for example by differentiating between harmful content itself and unproblematic references to it, such as may be found on scientific websites);
- iii. facilitate and promote initiatives that assist parents and educators in the selection and use of developmental-age appropriate filters for children and young people;
- iv. inform children and young people about the benefits and dangers of Internet content and its filtering as part of media education strategies in formal and non-formal education.

Furthermore, the private sector should be encouraged to:

- i. develop “intelligent” filters offering developmental-age appropriate filtering which can be adapted to follow the child’s progress and age while, at the same time, ensuring that filtering does not occur when the content is deemed neither harmful nor unsuitable for the group which the filter has been activated to protect;
- ii. co-operate with self- and co-regulatory bodies in order to develop standards for developmental-age appropriate rating systems for content carrying a risk of harm, taking into account the diversity of cultures, values and opinions;
- iii. develop, in co-operation with civil society, common labels for filters to assist parents and educators in making informed choices when acquiring filters and to certify that they meet certain quality requirements;
- iv. promote the interoperability of systems for the self-classification of content by providers and help to increase awareness about the potential benefits and dangers of such classification models.

Moreover, civil society should be encouraged to:

- i. debate and share their experiences and knowledge when assessing and raising awareness of the development and use of filters as a protective measure for children and young people;
- ii regularly monitor and analyse the use and impact of filters for children and young people, with particular regard to their effectiveness and their contribution to the exercise and enjoyment of the rights and freedoms guaranteed by Article 10 and other provisions of the European Convention on Human Rights.

### III. Use and application of Internet filters by the public and private sector

Notwithstanding the importance of empowering users to use and control filters as mentioned above, and noting the wider public service value of the Internet, public actors on all levels (such as administrations, libraries and educational institutions) which introduce filters or use them when delivering services to the public, should ensure full respect for all users’ right to freedom of expression and information and their right to private life and secrecy of correspondence.

In this context, member states should:

- i. refrain from filtering Internet content in electronic communications networks operated by public actors for reasons other than those laid down in Article 10, paragraph 2, of the European Convention on Human Rights, as interpreted by the European Court of Human Rights;
- ii. guarantee that nationwide general blocking or filtering measures are only introduced by the state if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled. Such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights;
- iii. introduce, where appropriate and necessary, provisions under national law for the prevention of intentional abuse of filters to restrict citizens' access to lawful content;
- iv. ensure that all filters are assessed both before and during their implementation to ensure that the effects of the filtering are proportionate to the purpose of the restriction and thus necessary in a democratic society, in order to avoid unreasonable blocking of content;
- v. provide for effective and readily accessible means of recourse and remedy, including suspension of filters, in cases where users and/or authors of content claim that content has been blocked unreasonably;
- vi. avoid the universal and general blocking of offensive or harmful content for users who are not part of the group which a filter has been activated to protect, and of illegal content for users who justifiably demonstrate a legitimate interest or need to access such content under exceptional circumstances, particularly for research purposes;
- vii. ensure that the right to private life and secrecy of correspondence is respected when using and applying filters and that personal data logged, recorded and processed via filters are only used for legitimate and non-commercial purposes.

Furthermore, member states and the private sector are encouraged to:

- i. regularly assess and review the effectiveness and proportionality regarding the introduction of filters;
- ii. strengthen the information and guidance to users who are subject to filters in private networks, including information about the existence of, and reasons for, the use of a filter and the criteria upon which the filter operates;
- iii. co-operate with users (customers, employees, etc.) to improve the transparency, effectiveness and proportionality of filters.

In this context, civil society should be encouraged to follow the development and deployment of filters both by key state and private sector actors. It should, where appropriate, call upon member states and the private sector, respectively, to ensure and to facilitate all users' right to

freedom of expression and information, in particular as regards their freedom to receive information without interference by public authorities and regardless of frontiers in the new information and communications environment.

### APPENDIX III

#### **Guidelines to assist online games providers in their practical understanding of, and compliance with, human rights and fundamental freedoms in the Information Society, in particular with regard to Article 10 of the European Convention on Human Rights**

##### **Background and context**

1. As part of its terms of reference, the Group of Specialists on Human Rights in the Information Society (MC-S-IS) was instructed by the Steering Committee on the Media and New Communications Services (CDMC) to develop tools to assist key state and non-state actors in their practical understanding of, and compliance with, human rights and fundamental freedoms in the information society, in particular with regard to Article 10 of the European Convention on Human Rights.
2. In response to its terms of reference, the MC-S-IS decided to develop human rights guidelines addressed to key actors with the aim of providing simple and practical advice relevant to the day-to-day activities of certain key actors, in this case online games providers.
3. To strengthen the practical nature of the guidelines, the MC-S-IS established contact with and has cooperated closely with ISFE, the Interactive Software Federation of Europe. ISFE has commented on the draft guidelines at various stages of their development and a meeting with participation of representatives of ISFE, a games producer as well as Council of Europe experts and Secretariat was organised. Moreover, ISFE was represented during the discussions of the draft guidelines at the 9th meeting of the MC-S-IS. The MC-S-IS aims to continue this positive co-operation after the text is finalised to maximise the impact and awareness of the guidelines among online games providers.
4. Based on existing Council of Europe standard-setting instruments, these guidelines are different from the existing Council of Europe instruments by being addressed directly to online games providers in order to raise awareness of the human rights aspects of their day-to-day work and activities. They are not binding on online games providers, rather they are a source of information and guidance for them to deal with practical issues concerning privacy, security and freedom of expression.
5. The guidelines are divided into three parts: (i) the role and position of online games providers vis-à-vis human rights in the information society; (ii) practical guidelines for online games providers containing advice and assistance; (iii) extracts from Council of Europe standard setting documents relevant to online games.



## **Human rights guidelines for online games providers**

Everyone has the right to freedom of expression and information. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Article 10 of the European Convention on Human Rights

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 of the European Convention on Human Rights

### **Understanding the role and position of online games providers in respecting and promoting human rights**

6. Providers (designers and publishers) of online games design and make available products which can promote the exercise and enjoyment of human rights and fundamental freedoms, in particular the freedom to express, to create and to exchange content and communications while respecting the rights of others. Designed and provided in an appropriate manner, games can be powerful tools to enhance learning, creativity and social interaction, thereby helping users to benefit from the information society.

7. However like other content, online games, may also inadvertently impact on the rights and sensibilities of individuals, in particular children, as well as their dignity. The potential impact of such games may increase as they allow the gaming experience to become more

creative and interactive (as the possibilities for expression, interaction and exchange of content with other gamers increase) and ever more realistic (as the visual effects of games develop).

8. Online games can play an important positive role in the lives and development of individuals, especially for children and young people. It suffices to consider the importance of rights and freedoms, values and dignity, into the embedded design and marketing of games. In this regard, it is recalled that the exercise of freedom of expression carries with it duties and responsibilities, in particular as regards the protection of health and morals and the rights of others, which publishers of online games are encouraged to bear in mind when deciding on the content of their games.

9. Games designers and publishers are therefore encouraged to promote and facilitate gamers' well-being and should regularly assess and evaluate their information policies and practices, in particular regarding child safety and responsible use, while respecting fundamental rights, in particular the right to freedom of expression and the right to privacy and secrecy of correspondence. At the same time it should be noted that member states, civil society, other private sector actors, parents and gamers themselves have important roles to play in engaging in multi-stakeholder cooperation, promoting gaming literacy for children and assisting game providers in fulfilling their role.

10. In this regard, designers and publishers of online games are encouraged to take note of, discuss and make their best efforts to comply with the following guidelines (below) and to consider making reference to them within their games and in their end-user agreements.

11. The appended guidelines are without prejudice to and must be read in conjunction with the obligations applicable to online games providers and their activities under national, European and international law.

#### Scope of the guidelines

12. The main focus of the following guidelines is online games although some of the guidelines can also be applied to games which are only playable offline. These online games include (i) classic board and card games mostly offered by web portals; (ii) personal computer (PC) or console games with network options; (iii) multiplayer games i.e. Massively Multiplayer Online Games where players play individually or in teams in a virtual evolving world, and (iv) entertainment games that provide a platform for other types of learning, training and interactive applications.

It should be noted that these guidelines are applicable to all online games irrespective of the platform used for delivery of the gaming content (fixed or mobile gaming console, PC or mobile phone).

13. These guidelines are mainly directed towards developers and publishers of online games. Some guidelines, such as those concerning the development of parental control tools, may also be applied by producers of gaming consoles and platforms in their activities.

14. Although online virtual universes, such as Second Life, are confronted with some of the same issues connected with online social interaction as games, they are, for the purposes of these guidelines, not seen as online games. In comparison with online games, such

universes only to a lesser degree constitute a programmed experience under the control of a game publisher. Virtual universes also lack a specified gaming scenario and set of goals to achieve for the gamer, characteristics which are normally found in online video games.

15. Finally, the guidelines are not intended to apply to online gambling sites, such as online casino or online bookmaking websites.

## **Guidelines**

**16** Before publishing your game, take care to consider and evaluate how the game content may impact on human dignity, the sensibilities and values of gamers, in particular children. In this regard specific attention should be paid to the risks connected with the dissemination of the following gaming content:

- Gratuitous portrayal of violence (physical, mental or sexual violence), especially in games targeting minors whose physical, mental or moral development may be impaired by exposure to such portrayal;
- Other content which, on account of its inhuman, cruel, sexist or degrading nature, may impact on the physical, mental or moral development of minors;
- Content which may be seen as advocating criminal or harmful behaviour (theft, violence, sale and abuse of drugs etc.);
- Content which conveys messages of aggressive nationalism, ethnocentrism, xenophobia, racism or intolerance in general including when such messages are concealed;

17. Consider promoting and applying independent, including combined, labelling and rating systems to your game, especially the Pan European Game Information (PEGI) system and the PEGI Online Safety Code (POSC), to help inform gamers, parents and carers about games containing content which may affect their sensibilities and values, in particular by:

- using easily recognisable labels for sensitive content (for example using symbols or pictograms), in particular with regard to violence, sex, racism, references to drugs, strong language, horror, or gambling;
- ensuring that such labels are clearly indicated and visible on the packaging of games and the game website, as well as in the references to them such as in catalogues, advertisements and in the materials provided with the game itself.

18. When publishing games targeted for children and young people, provide appropriate information to gamers, parent and carers of the risks connected with online gaming. Such information, which should be available in the local language of the country where the game is marketed and could usefully be provided in an educational guide written for parents, in the game manual and/or the game itself, may in particular concern:

- The risk of excessive use of online games and the potential negative physical and psychological effects of such excessive use (e.g. isolation, loss of the sense of reality, disturbed sleep patterns, etc.);

- The fact that the game is a work of fiction which can be a simulation of reality but is not comparable to the real world, and therefore that actions and behaviors in the game should not necessarily be re-enacted in the real lives of gamers;
- The risk of encountering illegal or harmful content uploaded by other gamers when playing the game online, and information and guidance for parents and carers on where to report the existence of such content within the game;
- The risk of harm associated with interaction with other gamers (for example with regard to bullying, harassment or stalking), and information and guidance about how to identify and deal with such risks;
- The risks to privacy of exchanging personal data (name, address, credit card details, images or videos) when playing the game online.

19. Consider developing in-game parental control tools to assist parent and carers in protecting minors. Such parental control tools could include facilities for setting time-limits and slots for gaming thereby limiting the risks of excessive use and addiction. If the parental tool include the option of filtering or blocking certain content, make sure that the filtering process is transparent both to the parent and gamer and can be adjusted to the level of protection required for the individual gamer, in accordance with the guidelines in the Council of Europe Recommendation [CM/Rec \(2008\)6](#) on measures to promote the respect for freedom of expression and information with regard to Internet filters.

20. Consider developing in-game mechanisms allowing gamers encountering illegal or harmful content or behaviour easy access to a facility to report the problems encountered, notify a game moderator and seek assistance.

21. Before removing gamer-generated content from a game, you should take care to verify the illegality or harmfulness of the content, for instance by contacting the competent authority law enforcement authorities. Acting without first checking and verifying may be considered as an interference with legal content and with the rights and freedoms of those gamers creating and communicating such content, in particular the right to freedom of expression and information.

22. Consider developing mechanisms for the automatic removal of gamer-generated content after a certain time of inactivity, in particular for games targeting children and young people. Creating a lasting or permanently accessible online record of the content created by gamers could challenge their dignity, security and privacy or otherwise render them vulnerable now or at a later stage in their lives.

23. Provide gamers with clear information about the presence of advertisements or product placements within the game along the lines of the principles contained in Article 10 of the PEGI Online Safety Code. When the game is targeted for minors, ensure that the content of advertisements and product placements is appropriate having regard to the age of the target group. As far as in-game advertising is concerned, make sure that there is no confusion between games for children and games for adults by respecting the labelling of the game, in particular by not including advertising for or clips from games treating mature subjects in childrens' games.

## Appendix I

### Extracts from existing Council of Europe standards relevant to the roles and responsibilities of games providers

#### Recommendation No. R (92)19 on video games with a racist content

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members, particularly for the purpose of safeguarding and realising the ideals and principles which are their common heritage;

Being aware that video games with a racist content, whose existence in member countries is unfortunately beyond doubt, convey a message of aggressive nationalism, ethnocentrism, xenophobia, anti-Semitism or intolerance in general, concealed behind or combined with violence or mockery;

Considering therefore that such games cannot be tolerated in democratic societies, which respect inter alia the right to be different, whether that difference be racial, religious or other;

Convinced that it is all the more necessary to take measures designed to put an end to the production and distribution of these games as they are used mainly by young people;

Recalling the terms of its Resolution (68) 30 relating to measures to be taken against incitement to racial, national and religious hatred and its Resolution (72) 22 on the suppression of and guaranteeing against unjustifiable discrimination;

Bearing in mind the Declaration regarding intolerance – a threat to democracy which it adopted on 14 May 1981;

Having regard to Recommendation No. R (89) 7 concerning principles on the distribution of videograms having a violent, brutal or pornographic content, and the European Convention on Transfrontier Television (European Treaty Series, No. 132),

Recommends that the governments of member states:

a. review the scope of their legislation in the fields of racial discrimination and hatred, violence and the protection of young people, in order to ensure that it applies without restriction to the production and distribution of video games with a racist content;

b. treat video games as mass media for the purposes of the application inter alia of Recommendation No. R (89) 7 concerning principles relating to the distribution of videograms having a violent, brutal or pornographic content, and of the European Convention on Transfrontier Television (European Treaty Series, No. 132).

**Recommendation No. R (97)19 on the portrayal of violence in the electronic media**

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and realising the ideals and principles which are their common heritage;

Recalling its commitment to the fundamental right to freedom of expression as guaranteed by Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, and to the principles of the free flow of information and ideas and the independence of media operators as expressed, in particular, in its Declaration on the freedom of expression and information of 29 April 1982;

Bearing in mind the international dimension of the gratuitous portrayal of violence and the relevant provisions of the European Convention on Transfrontier Television (1989);

Recalling that at the 4th European Ministerial Conference on Mass Media Policy (Prague, 7-8 December 1994), the Ministers responsible for media policy addressed to the Committee of Ministers of the Council of Europe an Action plan containing strategies for the promotion of the media in a democratic society, in which they requested the Committee of Ministers to "prepare, in close consultation with media professionals and regulatory authorities, possible guidelines on the portrayal of violence in the media";

Recalling that the exercise of freedom of expression carries with it duties and responsibilities, which media professionals must bear in mind, and that it may legitimately be restricted in order to maintain a balance between the exercise of this right and the respect for other fundamental rights, freedoms and interests protected by the European Convention on Human Rights;

Concerned at the overall increase in the portrayal of violence in the electronic media, which makes it an important social issue;

Recalling that violence cannot be considered a proper means for conflict-resolution of any kind, including inter-personal conflicts;

Noting, nevertheless, that violence is part of the daily reality of society and that the right of the public to be informed also covers the right to be informed about various manifestations of violence;

Noting that there are many ways in which violence may be portrayed by the media, corresponding to different contexts, ranging from information to entertainment and that, especially in the latter case, violence is sometimes trivialised or even glorified so as to attract large audiences;

Noting also that, regardless of the aim invoked, violence is sometimes portrayed in the electronic media in a gratuitous manner, in no way justified by the context, reaching unacceptable inhuman and degrading levels as well as an excessive overall volume;

Aware that this may impair the physical, mental or moral development of the public, particularly young people, by creating, for instance, growing insensitivity to suffering, feelings of insecurity and mistrust;

Noting that not all persons in charge of the various electronic media perceive the increased portrayal of violence as a problem;

Considering that the economic reasons advanced by certain persons in charge of electronic media cannot justify the gratuitous portrayal of violence;

Convinced that the various sectors of society should assume their responsibilities in regard to the portrayal of violence in the electronic media;

Convinced also that all electronic media professionals must assume their responsibilities and that they are best placed to address the question of gratuitous portrayal of violence; and welcoming efforts already made by certain professionals and sectors,

Recommends that the governments of the member States:

*a.* draw the attention of the professionals in the electronic media sector, the regulatory bodies for this sector, the educational authorities and the general public, to the overall policy framework represented by the appended guidelines;

*b.* take concrete measures to implement these;

*c.* ensure, by all appropriate means, that these guidelines are known by the persons and bodies concerned, and encourage general debate on this subject;

*d.* keep the effective application of them in their internal legal orders under review.

Instructs the Secretary General of the Council of Europe to transmit this recommendation to the governments of those States party to the European Cultural Convention which are not members of the Council of Europe.

### *Scope*

This recommendation concerns the gratuitous portrayal of violence in the various electronic media at national and transfrontier level. The gratuitous nature is to be assessed with reference to the parameters contained in the appendix to this recommendation.

### *Definitions*

For the purposes of this recommendation:

*a.* the term "gratuitous portrayal of violence" denotes the dissemination of messages, words and images, the violent content or presentation of which is given a prominence which is not justified in the context;

*b.* the term "electronic media" denotes radio and television programme services, services such as video-on-demand, Internet, interactive television, and so on, and products such as video

games, CD-ROMs, and so on, with the exception of private communications which are not accessible to the public;

c. the term "those responsible for the content" denotes natural or legal persons responsible for the content of messages, words and images made available to the public by the various electronic media.

### Guidelines

#### *Guideline No. 1 - General framework*

Article 10 of the European Convention on Human Rights, as interpreted in the case-law of the European Court of Human Rights, must constitute the general legal framework for addressing questions concerning the portrayal of violence in the electronic media.

Freedom of expression also includes, in principle, the right to impart and receive information and ideas which constitute portrayal of violence. However, certain forms of gratuitous portrayal of violence may lawfully be restricted, taking into account the duties and responsibilities which the exercise of freedom of expression carries with it, provided that such interferences with freedom of expression are prescribed by law and are necessary in a democratic society.

More specifically, measures taken to counter gratuitous portrayal of violence in the electronic media may legitimately aim at upholding respect for human dignity and at the protection of vulnerable groups, such as children and adolescents, whose physical, mental or moral development may be impaired by exposure to such portrayal.

#### *Guideline No. 2 - Responsibilities and means of action of non-State actors*

##### *Those responsible for the content*

Member States should recognise and take into account that it is first and foremost for those responsible for the content to assume the duties and responsibilities which the exercise of their freedom of expression entails, since they have primary responsibility for the content of the messages, words and images they disseminate. In particular, operators of electronic media have certain responsibilities when they decide to disseminate messages, words and images portraying violence, in view of the potentially harmful effects on the public, especially young people, as well as on society as a whole. These responsibilities have been assumed by media professionals in various ways, depending on the kind of electronic media, including, for example:

- i. ensuring, through appropriate means, that the public is made sufficiently aware in advance of messages, words and images of a violent content which they will make available;
- ii. the establishment of sectoral codes of conduct which specify the concrete responsibilities of the professional sector concerned;
- iii. the establishment of internal guidelines, including standards for evaluating content, in the various electronic media enterprises;



- iv. the establishment, at both sectoral level and within individual media enterprises, of appropriate consultation and control mechanisms for *monitoring* the implementation of self-regulatory standards;
- v. taking self-regulatory standards into account in contracts with other sectors, such as audio-visual producers, manufacturers of video games, advertising agencies, and so on;
- vi. regular contacts and exchange of information with national regulatory authorities, as well as with self-regulatory authorities, in other countries.

#### *The various sectors of society*

Member States should recognise and take into account the fact that various sectors of society have responsibilities in their own fields of activity. They may assume their responsibilities in various ways, for example by approaching those responsible for the content, in particular by awareness-raising campaigns; by promoting and providing media education; by promoting or undertaking research on the portrayal of violence, and so on.

As regards access to and the use of electronic media by children and adolescents at home and at school, as well as with respect to their understanding of violent messages, words and images transmitted by these media, parents and teachers have a special responsibility. They may assume this responsibility in various ways, including by:

- i. developing and maintaining a critical attitude towards the gratuitous portrayal of violence;
- ii. using the electronic media in a conscious and selective manner, as well as by demanding quality products and services;
- iii. stimulating children and adolescents to develop a critical attitude, for example through media education within the family and in schools;
- iv. examining ways of restricting access of children and adolescents to the violence portrayed in the electronic media where this is likely to impair the latter's physical, mental or moral development.

#### *Guideline No. 3 - Responsibilities and means of action of member States*

Member States bear general responsibility for, *inter alia*, the well-being of their population, for protecting human rights and for upholding respect for human dignity. However, as concerns the gratuitous portrayal of violence in the electronic media, member States only bear subsidiary responsibility, since the primary responsibility lies with those responsible for the content.

#### *National media policy*

Member States should adopt a global approach which is not limited to those responsible for the content but addresses the professional and social sectors concerned as a whole. This approach should, where appropriate, aim to:

- i. promote the establishment of independent regulatory authorities for the various electronic media. These authorities should be endowed with appropriate competence and means for regulating the portrayal of violence at national level;
- ii. enable electronic media consumers, both national and foreign, who criticise the violent content of certain services or products, to lodge a complaint with the regulatory authority or another competent national body;
- iii. include among the licensing conditions for broadcasters certain obligations concerning the portrayal of violence, accompanied by dissuasive measures of an administrative nature, such as non-renewal of the licence when these obligations are not respected;
- iv. establish methods to facilitate the division of responsibilities between those responsible for the content and the public (warnings, "watersheds", and so on);
- v. raise the electronic media professionals' awareness of the problems connected with the gratuitous portrayal of violence and the public's concern about them;
- vi. promote research on the portrayal of violence in the electronic media, in particular on trends in the various media, and studies of the effects of such portrayal on the public.

#### *International co-operation*

In addition to their existing international obligations and activities carried out within the framework of the Council of Europe, member States should co-operate bilaterally and multilaterally as well as within the framework of competent international organisations, with a view to developing policies for addressing problems related, in particular, to the international dimension of the gratuitous portrayal of violence in the electronic media.

In this respect, they should facilitate the exchange of information and co-operation between competent regulatory authorities, in particular as concerns content classification and the handling of any complaints lodged from abroad.

#### *Legal measures*

Where those responsible for the content engage in the gratuitous portrayal of violence which grossly offends human dignity or which, on account of its inhuman or degrading nature, impairs the physical, mental or moral development of the public, particularly young people, member States should effectively apply relevant civil, criminal or administrative sanctions.

Member States which are not yet Parties to the European Convention on Transfrontier Television (1989) are invited to accede to this instrument. All States Parties to the Convention should ensure its effective implementation, in particular as concerns the provisions dealing with the portrayal of violence, and regularly evaluate its effectiveness. Member States are also invited to give an appropriate follow-up to Recommendation No. R (89) 7 of the Committee of Ministers on principles on the distribution of videograms having a violent, brutal or pornographic content.

#### *Promotion of non-violent quality programmes, services and products*

Within the framework in particular of the various national and European programmes of support for the production and distribution of audio-visual works, and in close co-operation with European bodies and professional circles concerned, member States should promote the principle of non-violent quality programmes, services and products which reflect the cultural diversity and richness of European countries.

*Guideline No. 4 - Shared responsibility for electronic media education*

States should consider electronic media education as a responsibility shared between themselves, those responsible for the content and the various sectors of society. Such education constitutes a particularly appropriate way of helping the public, especially the young, to develop a critical attitude in regard to different forms of portrayal of violence in these media and to make informed choices.”

**Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet<sup>6</sup>**

The Committee of Ministers of the Council of Europe,

Recalling the fundamental right to freedom of expression and to receive and impart information and ideas without interference by public authorities and regardless of frontiers, as guaranteed by Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights – ETS No. 5);

Recalling the 1989 United Nations Convention of the Rights of the Child, in particular the inherent right for children to dignity, to special protection and care as is necessary for their well-being, to protection against all forms of discrimination or arbitrary or unlawful interference with their privacy and to unlawful attacks on their honour and reputation;

Convinced that the well-being and best interests of children are fundamental values shared by all member states, which must be promoted without any discrimination;

Convinced that the Internet is an important tool for children’s everyday activities, such as communication, information, knowledge, education and entertainment;

Concerned however by the enduring presence of content created by children which can be damaging to their dignity, security, privacy and honour both now and in the future as adults;

Recalling the Committee of Ministers’ Declaration on freedom of communication on the Internet, adopted on 28 May 2003, which stresses that the exercise of such freedom should not prejudice the dignity or fundamental rights and freedoms of others, especially children;

Conscious that the traceability of children’s activities via the Internet may expose them to criminal activities, such as the solicitation of children for sexual purposes, or otherwise illegal or harmful activities, such as discrimination, bullying, stalking and other forms of harassment, by others;

---

<sup>6</sup> Adopted on 20 February 2008.

Recalling the measures to protect children referred to in the 2001 Convention on Cybercrime (ETS No. 185), in particular concerning child pornography, and the 2007 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201), in particular concerning the solicitation of children for sexual purposes;

Convinced of the need to inform children about the enduring presence and risks of the content they create on the Internet and, in this connection, of the need to develop and promote their information literacy, defined as the competent use of tools providing access to information, the development of critical analysis of content and the appropriation of communication skills to foster citizenship and creativity, as referred to in Recommendation Rec(2006)12 of the Committee of Ministers on empowering children in the new information and communications environment;

Aware that communication using new technologies and new information and communication services must respect the right to privacy and to secrecy of correspondence, as guaranteed by Article 8 of the European Convention on Human Rights and as elaborated by the case law of the European Court of Human Rights, as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108);

Concerned by the profiling of information and the retention of personal data regarding children's activities for commercial purposes;

Noting the outcome documents of the United Nations World Summit on the Information Society (Geneva, 2003 – Tunis, 2005), in particular the 2005 Tunis Agenda for the Information Society which reaffirmed the commitment to effective policies and frameworks to protect children and young people from abuse and exploitation through information and communication technologies;

Noting also the mandate of the United Nations Internet Governance Forum, in particular to identify emerging issues regarding the development and security of the Internet and to help find solutions to the issues arising from the use and misuse of the Internet, of concern to everyday users;

Aware of the emerging tendency for certain types of institutions, such as educational establishments, and prospective employers to seek information about children and young people when deciding on important issues concerning their lives,

Declares that, other than in the context of law enforcement, there should be no lasting or permanently accessible record of the content created by children on the Internet which challenges their dignity, security and privacy or otherwise renders them vulnerable now or at a later stage in their lives;

Invites member states together, where appropriate, with other relevant stakeholders, to explore the feasibility of removing or deleting such content, including its traces (logs, records and processing), within a reasonably short period of time.

**Recommendation No. CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters**

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve greater unity between its members for the purpose of safeguarding and realising the ideals and principles which are their common heritage;

Recalling that States Parties to the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights – ETS No. 5) have undertaken to secure to everyone within their jurisdiction the human rights and fundamental freedoms defined in the Convention;

Reaffirming the commitment of member states to the fundamental right to freedom of expression and to receive and impart information and ideas without interference by public authorities and regardless of frontiers, as guaranteed by Article 10 of the European Convention on Human Rights;

Aware that any intervention by member states that forbids access to specific Internet content may constitute a restriction on freedom of expression and access to information in the online environment and that such a restriction would have to fulfil the conditions in Article 10, paragraph 2, of the European Convention on Human Rights and the relevant case law of the European Court of Human Rights;

Recalling in this respect the Declaration on human rights and the rule of law in the information society, adopted by the Committee of Ministers on 13 May 2005, according to which member states should maintain and enhance legal and practical measures to prevent state and private censorship;

Recalling Recommendation Rec(2007)11 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment, according to which member states, the private sector and civil society are encouraged to develop common standards and strategies to promote transparency and the provision of information, guidance and assistance to the individual users of technologies and services concerning, *inter alia*, the blocking of access to and filtering of content and services with regard to the right to receive and impart information;

Noting that the voluntary and responsible use of Internet filters (products, systems and measures to block or filter Internet content) can promote confidence and security on the Internet for users, in particular children and young people, while also aware that the use of such filters can impact on the right to freedom of expression and information, as protected by Article 10 of the European Convention on Human Rights;

Recalling Recommendation [Rec\(2006\)12](#) of the Committee of Ministers on empowering children in the new information and communications environment, which underlines the importance of information literacy and training strategies for children to enable them to better understand and deal with content (for example violence and self-harm, pornography,

discrimination and racism) and behaviours (such as grooming, bullying, harassment or stalking) carrying a risk of harm, thereby promoting a greater sense of confidence, well-being and respect for others in the new information and communications environment;

Convinced of the necessity to ensure that users are made aware of, understand and are able to effectively use, adjust and control filters according to their individual needs;

Recalling Recommendation [Rec\(2001\)8](#) of the Committee of Ministers on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), which encourages the neutral labelling of content to enable users to make their own value judgements over such content and the development of a wide range of search tools and filtering profiles, which provide users with the ability to select content on the basis of content descriptors;

Aware of the public service value of the Internet, understood as people's significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions, entertainment) and the resulting legitimate expectation that Internet services be accessible, affordable, secure, reliable and ongoing and recalling in this regard Recommendation Rec(2007)16 of the Committee of Ministers on measures to promote the public service value of the Internet;

Recalling the Declaration of the Committee of Ministers on freedom of communication on the Internet of 28 May 2003, which stresses that public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers, but that this does not prevent the installation of filters for the protection of minors, in particular in places accessible to them, such as schools or libraries;

Reaffirming the commitment of member states to everyone's right to private life and secrecy of correspondence, as protected by Article 8 of the European Convention on Human Rights, and recalling the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and its Additional Protocol regarding supervisory authorities and transborder data flows (ETS No. 181) as well as Recommendation No. R (99) 5 of the Committee of Ministers on the protection of privacy on the Internet,

Recommends that member states adopt common standards and strategies with regard to Internet filters to promote the full exercise and enjoyment of the right to freedom of expression and information and related rights and freedoms in the European Convention on Human Rights, in particular by:

- taking measures with regard to Internet filters in line with the guidelines set out in the appendix to this recommendation;

- bringing these guidelines to the attention of all relevant private and public sector stakeholders, in particular those who design, use (install, activate, deactivate and implement) and monitor Internet filters, and to civil society, so that they may contribute to their implementation.

*Appendix to Recommendation CM/Rec(2008)6**Guidelines*I. Using and controlling Internet filters in order to fully exercise and enjoy the right to freedom of expression and information

Users' awareness, understanding of and ability to effectively use Internet filters are key factors which enable them to fully exercise and enjoy their human rights and fundamental freedoms, in particular the right to freedom of expression and information, and to participate actively in democratic processes. When confronted with filters, users must be informed that a filter is active and, where appropriate, be able to identify and to control the level of filtering the content they access is subject to. Moreover, they should have the possibility to challenge the blocking or filtering of content and to seek clarifications and remedies.

In co-operation with the private sector and civil society, member states should ensure that users are made aware of activated filters and, where appropriate, are able to activate and deactivate them and be assisted in varying the level of filtering in operation, in particular by:

- i. developing and promoting a minimum level of information for users to enable them to identify when filtering has been activated and to understand how, and according to which criteria, the filtering operates (for example, black lists, white lists, keyword blocking, content rating, etc., or combinations thereof);
- ii. developing minimum levels of and standards for the information provided to the user to explain why a specific type of content has been filtered;
- iii. regularly reviewing and updating filters in order to improve their effectiveness, proportionality and legitimacy in relation to their intended purpose;
- iv. providing clear and concise information and guidance regarding the manual overriding of an activated filter, namely whom to contact when it appears that content has been unreasonably blocked and the reasons which may allow a filter to be overridden for a specific type of content or Uniform Resource Locator (URL);
- v. ensuring that content filtered by mistake or error can be accessed without undue difficulty and within a reasonable time;
- vi. promoting initiatives to raise awareness of the social and ethical responsibilities of those actors who design, use and monitor filters with particular regard to the right to freedom of expression and information and to the right to private life, as well as to the active participation in public life and democratic processes;
- vii. raising awareness of the potential limitations to freedom of expression and information and the right to private life resulting from the use of filters and of the need to ensure proportionality of such limitations;
- viii. facilitating an exchange of experiences and best practices with regard to the design, use and monitoring of filters;

- ix. encouraging the provision of training courses for network administrators, parents, educators and other people using and monitoring filters;
- x. promoting and co-operating with existing initiatives to foster responsible use of filters in compliance with human rights, democracy and the rule of law;
- xi. fostering filtering standards and benchmarks to help users choose and best control filters.

In this context, civil society should be encouraged to raise users' awareness of the potential benefits and dangers of filters. This should include promoting the importance and significance of free and unhindered access to the Internet so that every individual user may fully exercise and enjoy their human rights and fundamental freedoms, in particular the right to freedom of expression and information and the right to private life, as well as to effectively participate in public life and democratic processes.

## II. Appropriate filtering for children and young people

The Internet has significantly increased the number and diversity of ideas, information and opinions which people may receive and impart in the fulfilment of their right to freedom of expression and information without interference by public authorities and regardless of frontiers. At the same time, it has increased the amount of readily available content carrying a risk of harm, particularly for children and young people. To satisfy the legitimate desire and duty of member states to protect children and young people from content carrying a risk of harm, the proportionate use of filters can constitute an appropriate means of encouraging access to and confident use of the Internet and be a complement to other strategies on how to tackle harmful content, such as the development and provision of information literacy.

In this context, member states should:

- i. facilitate the development of strategies to identify content carrying a risk of harm for children and young people, taking into account the diversity of cultures, values and opinions;
- ii. co-operate with the private sector and civil society to avoid over-protection of children and young people by, *inter alia*, supporting research and development for the production of "intelligent" filters that take more account of the context in which the information is provided (for example by differentiating between harmful content itself and unproblematic references to it, such as may be found on scientific websites);
- iii. facilitate and promote initiatives that assist parents and educators in the selection and use of developmental-age appropriate filters for children and young people;
- iv. inform children and young people about the benefits and dangers of Internet content and its filtering as part of media education strategies in formal and non-formal education.

Furthermore, the private sector should be encouraged to:

- i. develop "intelligent" filters offering developmental-age appropriate filtering which can be adapted to follow the child's progress and age while, at the same time, ensuring that filtering does not occur when the content is deemed neither harmful nor unsuitable for the group which the filter has been activated to protect;



- ii. co-operate with self- and co-regulatory bodies in order to develop standards for developmental-age appropriate rating systems for content carrying a risk of harm, taking into account the diversity of cultures, values and opinions;
- iii. develop, in co-operation with civil society, common labels for filters to assist parents and educators in making informed choices when acquiring filters and to certify that they meet certain quality requirements;
- iv. promote the interoperability of systems for the self-classification of content by providers and help to increase awareness about the potential benefits and dangers of such classification models.

Moreover, civil society should be encouraged to:

- i. debate and share their experiences and knowledge when assessing and raising awareness of the development and use of filters as a protective measure for children and young people;
- ii regularly monitor and analyse the use and impact of filters for children and young people, with particular regard to their effectiveness and their contribution to the exercise and enjoyment of the rights and freedoms guaranteed by Article 10 and other provisions of the European Convention on Human Rights.

### III. Use and application of Internet filters by the public and private sector

Notwithstanding the importance of empowering users to use and control filters as mentioned above, and noting the wider public service value of the Internet, public actors on all levels (such as administrations, libraries and educational institutions) which introduce filters or use them when delivering services to the public, should ensure full respect for all users' right to freedom of expression and information and their right to private life and secrecy of correspondence.

In this context, member states should:

- i. refrain from filtering Internet content in electronic communications networks operated by public actors for reasons other than those laid down in Article 10, paragraph 2, of the European Convention on Human Rights, as interpreted by the European Court of Human Rights;
- ii. guarantee that nationwide general blocking or filtering measures are only introduced by the state if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled. Such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights;
- iii. introduce, where appropriate and necessary, provisions under national law for the prevention of intentional abuse of filters to restrict citizens' access to lawful content;

iv. ensure that all filters are assessed both before and during their implementation to ensure that the effects of the filtering are proportionate to the purpose of the restriction and thus necessary in a democratic society, in order to avoid unreasonable blocking of content;

v. provide for effective and readily accessible means of recourse and remedy, including suspension of filters, in cases where users and/or authors of content claim that content has been blocked unreasonably;

vi. avoid the universal and general blocking of offensive or harmful content for users who are not part of the group which a filter has been activated to protect, and of illegal content for users who justifiably demonstrate a legitimate interest or need to access such content under exceptional circumstances, particularly for research purposes;

vii. ensure that the right to private life and secrecy of correspondence is respected when using and applying filters and that personal data logged, recorded and processed via filters are only used for legitimate and non-commercial purposes.

Furthermore, member states and the private sector are encouraged to:

i. regularly assess and review the effectiveness and proportionality regarding the introduction of filters;

ii. strengthen the information and guidance to users who are subject to filters in private networks, including information about the existence of, and reasons for, the use of a filter and the criteria upon which the filter operates;

iii. co-operate with users (customers, employees, etc.) to improve the transparency, effectiveness and proportionality of filters.

In this context, civil society should be encouraged to follow the development and deployment of filters both by key state and private sector actors. It should, where appropriate, call upon member states and the private sector, respectively, to ensure and to facilitate all users' right to freedom of expression and information, in particular as regards their freedom to receive information without interference by public authorities and regardless of frontiers in the new information and communications environment.